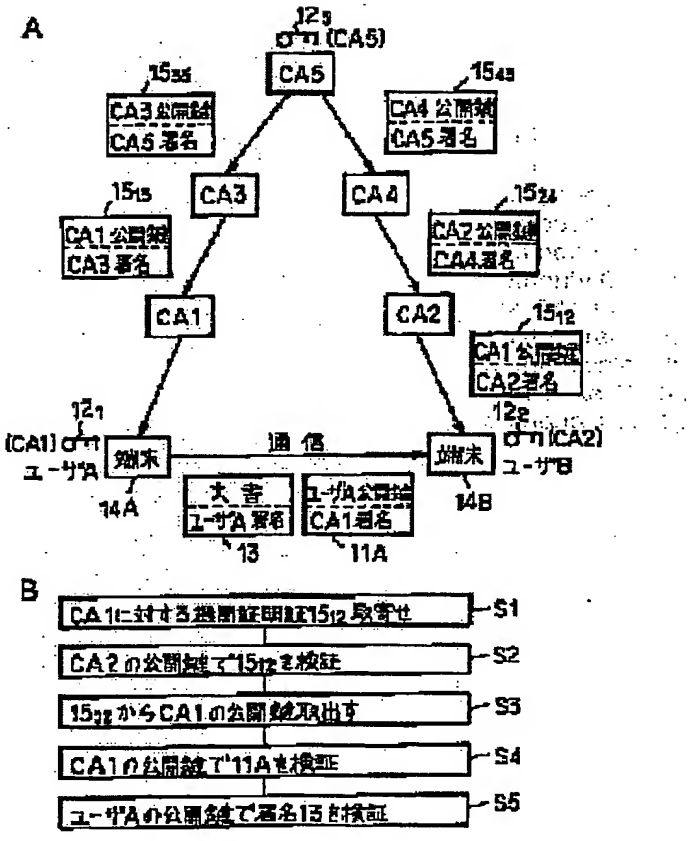
PUBLIC KEY AUTHENTICATION METHOD

Patent number:	JP10215245
Publication date:	1998-08-11
Inventor:	HASHIMOTO SHOICHI
Applicant:	NIPPON TELEGRAPH & TELEPHONE
Classification:	
- International:	H04L9/32
- european:	
Application number:	JP19970015463 19970129
Priority number(s):	JP19970015463 19970129

Abstract of **JP10215245**

PROBLEM TO BE SOLVED: To relieve the load of the user for authentication processing in the case that a certification authority issuing a public key certificate is different from the certification authority issuing the certificate for the user. SOLUTION: Once a certificate 11A authenticated by a certification authority CA1 has been received, a user B whose public key has been authenticated by a certification authority CA2 requests the authentication of the CA1 to the CA2. The CA2 traces the trusted tree structure of the CA1 and authenticates the validity of a signature in a certificate 1535 with respect to a certification authority CA3 by using a public key of a certification authority CA5 that is the highest certification authority, authenticates the validity of a signature in a certificate 1515 with respect to the certification authority CA1 by using a public key of the certification authority CA3. When the signature is successfully authenticated, the CA2 puts its public key as signature to the public key of the CA1 in the certificate 1513 , sends a certificate 1512 to the user B. The user B uses the public key of the CA2 to authenticate the certificate 1512 . When the signature is successfully authenticated, the user B uses the public key included in the certificate to authenticate a public key of a user A in the certificate 11A.



(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－２１５２４５

(43)公開日　平成10年(1998)8月11日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７５　Ｚ
				６７５　Ｄ

審査請求　未請求　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願平9-15463

(22)出願日　平成9年(1997)1月29日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者　橋本　正一
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】公開鍵認証方法

(57)【要約】

【課題】　公開鍵証明証を発行した証明機関が異なる場合のユーザの検証処理を軽減する。

【解決手段】　証明機関ＣＡ２により公開鍵を証明されているユーザＢがＣＡ１により証明された証明証１１Ａを受信すると、ＣＡ２にＣＡ１の検証を依頼する。ＣＡ２はＣＡ１の信頼関係木構造を辿って、最上位のＣＡ５の公開鍵でＣＡ３に対する証明証15_{35}の署名の正当性を検証し、ＣＡ３の公開鍵でＣＡ１に対する証明証15_{13}の署名の正当性を検証し、これらに合格すると15_{13}中のＣＡ１の公開鍵をＣＡ２の公開鍵で署名して証明証15_{12}をユーザＢへ送り、ユーザＢは、ＣＡ２の公開鍵で15_{12}を検証し、合格したらこれに含まれているＣＡ１公開鍵を用いて証明証１１Ａのユーザの公開鍵を検証する。

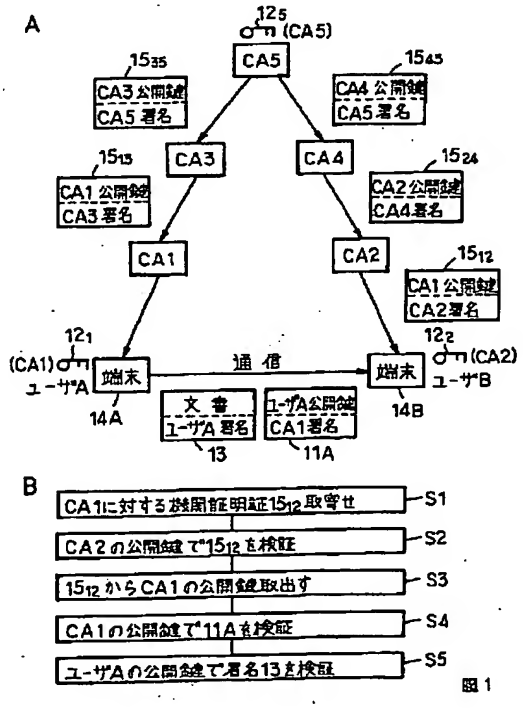


図1

1

【特許請求の範囲】

【請求項１】　公開鍵とその所有者との対応付けを保証して、公開鍵証明証を発行する証明機関が複数存在し、これら証明機関が木構造などの信頼関係により上位の証明機関がその下位の証明機関の公開鍵を保証した機関証明証を発行することを順次行っており、

利用者Ｂの端末（以下端末Ｂと記す）に受信された利用者Ａの公開鍵証明証Ａの発行証明機関Ａが、端末Ｂ（利用者Ｂ）に対する公開鍵証明証Ｂの発行証明機関Ｂと異なる場合に、

端末Ｂは証明機関Ｂに証明機関Ａを保証する機関証明証の発行を依頼し、

証明機関Ｂはその機関Ｂが証明機関Ａの公開鍵を保証した機関証明証を端末Ｂに送り、

端末Ｂは受信した機関証明証を検証し、合格すると、その機関証明証に含まれている証明機関Ａの公開鍵を用いて上記公開鍵証明証Ａの検証を行うことを特徴とする公開鍵認証方法。

【請求項２】　上記証明機関Ｂは上記証明機関Ａの公開鍵を保証した機関証明証の発行に際し、上記証明機関Ａの公開鍵をその上位の証明機関が保証した機関証明証により証明機関Ａの信頼性を検証し、この証明機関の信頼性の検証を順次上位の証明機関に対して行い、最上位の証明機関による保証の確認ができた場合に上記証明機関Ａの公開鍵を保証した機関証明証を発行することを特徴とする請求項１記載の公開鍵認証方法。

【請求項３】　上記証明機関の信頼性の認証が正しい場合にその入手した各機関証明証及び上記証明機関Ａに対して発行した機関証明証を記憶しておき、上記端末Ｂの機関証明証の発行依頼に対し、上記記憶した機関証明証を利用することを特徴とする請求項２記載の公開鍵認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は公開鍵暗号方式を用いた情報通信において、異なる証明機関から証明証が発行されているユーザ（利用者）間で通信を行う場合に、通信相手の証明証の正当性を効率的に確認し、安全に通信を行うための認証方法に関するものである。

【０００２】

【従来の技術】電子情報の送受信において、確かに送信者本人から送信されたものであるかということや、通信路において改ざんが行われていないかということなどを検知するための方法として公開鍵暗号方式が利用されている。この方式では、一般に広く公開しておく公開鍵と、自分のみが知り得る秘密鍵の２種類の鍵を用いて通信が行われる。ここで公開鍵を単に周知するだけでは他人を装って通知する「なりすまし」と呼ばれる脅威が考えられることから、証明機関が、公開鍵と所有者との関係を保証し、所有者の公開鍵証明証を発行する形態が一般に行われている。証明証には、ユーザ（利用者）の公開鍵および所有者に関する情報と、証明証を発行する証明機関の電子署名（以下ＣＡ署名と略す、ＣＡ：Certification Authority ）が付与されている。ユーザは、この証明機関の公開鍵を用いて通信相手の証明証のＣＡ署名を復号化処理することで、確かに当該証明機関が発行した証明証であることを検証し、通信相手の証明証に登録されている公開鍵を取り出して利用する。

2

【０００３】ここで検証に用いる証明機関の公開鍵は、通常、証明機関が証明証を発行したユーザに対して、安全な方法で配付されているため、同一の証明機関から証明証の発行を受けたユーザ同士が通信する場合には、配付されている証明機関の公開鍵によって通信相手の証明証の正当性を検証することができる。即ち図３に示すように、ユーザＡは利用する公開鍵とその所有者がユーザＡであることを証明機関ＣＡ１により署名したユーザＡの公開鍵証明証１１Ａを発行してもらう。ユーザＢも同様にしてユーザ公開鍵とその所有についての署名をしたユーザＢの公開鍵証明証１１Ｂを証明機関ＣＡ１により発行してもらう。同時にユーザＡ、ユーザＢに、証明証検証用の証明機関ＣＡ１の公開鍵12_1がそれぞれ安全な方法で配付されている。ユーザＡがユーザＡの署名を付けた文書１３をユーザＢへ送信する際に、まずユーザＡの公開鍵証明証１１Ａをユーザの端末１４Ａからユーザの端末１４Ｂへ送信する。ユーザＢの端末１４Ｂでは受信した証明証１１Ａを、証明機関ＣＡ１の公開鍵12_1によりそのユーザＡの公開鍵が証明機関ＣＡ１により認証されたものであるか否かを検証し、つまり公開鍵12_1で証明機関ＣＡ１の署名を復号化して公開鍵を復号し、その復号した公開鍵が、証明証１１Ａに示されているユーザＡの公開鍵と同一であるかを調べ、一致していれば、その公開鍵は証明機関ＣＡ１によりユーザＡのものであると保証されたものとして、その公開鍵を取り出して文書１３の署名を検証する。

【０００４】しかしながら、異なる証明機関から証明証が発行されているユーザ間で通信を行う場合には、通信相手の証明証に付与されたＣＡ署名を検証するための証明機関の公開鍵を持っていないため、通信相手の証明証の正当性を確認することができない。そこで通信相手の証明証を発行した証明機関が信頼できる証明機関であるかを確認するために、図４に示すように、上位の証明機関が下位の証明機関に対して証明証を発行することで、複数証明機関間における信頼関係の木構造を構築する。そして、「信頼できる証明機関が信頼している証明機関は信頼できる」という考えに基づいて、相手証明機関から、信頼の木構造を複数の証明機関を介しながら木構造全体から信頼されている最上位の証明機関ＣＡ５まで辿ることによって、相手証明機関の信頼性が確認できるようになる。

【０００５】例えば図４Ａに示すように、ユーザＡの公

開鍵に対する証明証１１Ａを発行した証明機関ＣＡ１の上位の証明機関ＣＡ３は証明機関ＣＡ１の公開鍵とその機関名ＣＡ１と、これに対するＣＡ３の署名とよりなる機関証明証15_{13}を発行し、証明機関ＣＡ３の上位の証明機関ＣＡ５は証明機関ＣＡ３の公開鍵およびその機関ＣＡ３と、これらに対するＣＡ５の署名とよりなる機関証明証15_{35}を発行する。証明機関ＣＡ５はこの例では最上位の機関である。同様にユーザＢに対し、公開鍵証明証１１Ｂを発行した証明機関ＣＡ２に対し、その上位の証明機関ＣＡ４は機関証明証15_{24}を発行し、証明機関ＣＡ４に対し、その上位証明機関ＣＡ５が機関証明証15_{45}を発行し、木構造の信頼関係が構成されている。

【０００６】ユーザ１４Ａがその署名付き文書１３をユーザＢへ送る際に、ユーザＡの公開鍵証明証１１Ａをユーザ Ｂへ送信しても、ユーザＢの端末１４Ｂは証明機関ＣＡ２の公開鍵12_2 しかもっていないから証明証１１Ａの正当性を検証することはできない、つまりユーザＡの公開鍵が信頼できるものか不明である。従ってユーザＢの端末１４Ｂは図４Ｂに示すように受信した証明証１１Ａの公開情報からその証明機関ＣＡ１とその上位機関ＣＡ３を知り、上位機関ＣＡ３が証明機関ＣＡ１に対し発行した機関証明証15_{13}の正当性を証明機関ＣＡ３の公開鍵で検証し、これに合格すれば、証明機関ＣＡ３の上位機関ＣＡ５が証明機関ＣＡ３に対して発行した機関証明証15_{35}の正当性を機関ＣＡ５の公開鍵12_5 で検証し、この検証に合格したら、証明機関ＣＡ３，ＣＡ１がそれぞれ信頼されるものであり、従って証明証１１Ａのユーザの公開鍵も信頼できるものと判定する。

【０００７】このように信頼性の確認の際には、木構造を辿る際に証明機関間で発行されている証明証を取り寄せて、下位証明機関の証明証に付与されている上位証明機関の署名を、その上位証明機関の証明証中にある公開鍵によって検証するということを順次最上位の証明機関ＣＡ５の公開鍵による検証が行われるまで繰り返し行うことによって、相手証明機関ＣＡ１の公開鍵の正当性を確認していた。

【０００８】

【発明が解決しようとする課題】自己の公開鍵証明証を発行している証明機関と異なる証明機関から発行されている通信相手の証明証の正当性を検証する場合、図４に示したように、証明機関間の信頼関係を示す木構造に対して、通信相手の証明証を発行した証明機関から最上位の証明機関までのパス上にある機関証明証をすべて取り寄せて、それぞれについて検証処理を行うため、木構造で辿るパスの数だけの証明証の検証処理回数が必要となり、ユーザにとって大きな負担となっていた。また、木構造の上位の証明機関ほど、ユーザからの証明証取得要求が集中するため、上位証明機関におけるユーザからのアクセス要求に対する処理負荷が大きくなっていた。そこで、ユーザが少ない検証処理回数で通信相手の証明証の正当性の確認及び特定の証明機関に対するユーザからのアクセス集中を回避する方法をこの発明は提案することを目的とする。

【０００９】

【課題を解決するための手段】この発明では、直接信頼の上下関係がなかったために証明証の発行が行われていなかった証明機関に対して、従来はユーザが木構造を辿りながら行っていた検証処理を証明機関が自ら行って、その証明機関の公開鍵の正当性を確認することで、これを証明機関間の間接認証としてその証明機関の公開鍵に対して機関証明証の発行を行う。

【００１０】つまりこの発明によれば、複数の証明機関間に木構造などの信頼関係が構成され、第１利用者の公開鍵であることを第１証明機関が保証した公開鍵証明証を第２利用者が受け取り、その公開鍵証明証を検証する際に、第２利用者の公開鍵を保証している第２証明機関が上記第１証明機関と直接的には信頼関係にない場合は、上記第２証明機関が上記第１証明機関の公開鍵の正当性の検証を行い、その検証結果を上記第１証明機関に対する機関証明証として発行し、第２利用者はその機関証明証内にある第２証明機関が正当と認めた第１証明機関の公開鍵を用いて第１利用者の公開鍵証明証の検証を行う。

【００１１】上記第２証明機関による第１証明機関の公開鍵の正当性の検証は、その第１証明機関の公開鍵を保証しているその上位の証明機関の機関証明証を検証し、更にその上位証明機関の公開鍵の正当性を更にその上位証明機関が発行しているその機関証明証を検証するというように順次木構造を辿って、最上位の証明機関が発行した機関証明証の検証まで行うことにより達成する。

【００１２】１度この検証を行い、正当であった場合は、その各機関証明証を第２証明機関に記憶しておき、他の証明機関の公開鍵の正当性を検証する場合に、まず、自己の証明機関内に、その他の証明機関の公開鍵を検証した機関証明証があるかを参照し、あればこれを用いる。

【００１３】

【発明の実施の形態】図１Ａにこの発明の実施例を適用したシステム例を示し、図４Ａと対応する部分に同一符号を付けてある。従来技術での説明例と同様に、ユーザＡが署名文書１３をユーザＢへ送るため、証明機関ＣＡ１が署名したユーザ公開鍵証明証１１Ａをユーザ Ｂの端末１４Ｂへ送信する。ユーザＢの端末１４Ｂでは受信した鍵証明証１１Ａは証明機関ＣＡ１が保証（署名）したものであるから、これの正当性を検証することはできない。

【００１４】そこでユーザＢの端末１４Ｂは証明機関ＣＡ１の公開鍵の信頼性検証を自己の証明機関ＣＡ２に依頼する。この依頼を受けた証明機関ＣＡ２は証明機関ＣＡ１からその信頼関係の木構造を辿って最上位の証明機

関ＣＡ５に達するまでのすべての証明機関の公開鍵検証に必要な機関証明証15_{13}，15_{36}を集め証明機関ＣＡ１の公開鍵に対する検証のために機関証明証15_{13}を機関証明証15_{36}内の証明機関ＣＡ３の公開鍵を用いて検証し、これに合格すると最上位証明機関ＣＡ５の公開鍵を用いて機関証明証15_{36}を検証する。

【００１５】この検証に合格すれば、証明機関ＣＡ１に対して発行されている機関証明証15_{13}から証明機関ＣＡ１の公開鍵及び公開情報（機関名称など）を取り出す。その取り出した証明機関ＣＡ１の公開鍵及び公開情報と、証明機関ＣＡ２のこれらに対する署名とにより機関証明証15_{12}を作り、これをユーザＢの端末１４Ｂへ送信する。

【００１６】以上のようにして端末１４Ｂは証明機関ＣＡ２が発行した証明機関ＣＡ１の公開鍵に対する機関証明証15_{12}を取得し（Ｓ１）、端末１４Ｂは図１Ｂに示すようにその機関証明証15_{12}を証明機関ＣＡ２の公開鍵12_2で検証し（Ｓ２）、合格したら、その機関証明証15_{12}に含まれている証明機関ＣＡ１の公開鍵を取り出し（Ｓ３）、これを用いて、ユーザＡの端末１４Ａから受信した公開鍵証明証１１Ａを検証し（Ｓ４）、これに合格すれば、その公開鍵証明証１１Ａに含まれているユーザＡの公開鍵を用いて受信した署名文書１３の検証を行う（Ｓ５）。

【００１７】証明機関ＣＡ２は以上のようにして証明機関ＣＡ１の公開鍵に対する機関証明証15_{12}を発行すると、これを記憶部に記憶しておき、同一の証明要求が発生した場合に、記憶した機関証明証を発行してもよい。また各検証済の機関証明証も記憶しておき、他の証明機関の公開鍵の検証で利用できるものは、それを利用して、検証処理を迅速化することもできる。証明機関ＣＡ１の公開鍵の正当性の検証は、機関証明証15_{36}を検証し、次に機関証明証15_{13}を検証するような順番としてもよい。

【００１８】次に証明機関、例えばＣＡ２が、これと直接信頼関係にない証明機関、例えばＣＡ１の公開鍵の正当性を検証し、その証明証を発行する手順を図２を参照して説明する。ユーザから、対象証明機関（例えばＣＡ１）の機関証明証発行依頼を受けると（Ｓ１）、その機関証明証について記憶部（データベース）２１を検索し（Ｓ２）、既に発行済みの機関証明証であれば、これを記憶部２１から読みだして、要求ユーザ端末へ送付する（Ｓ３）。

【００１９】発行済みのものがなければ、その対象証明機関の発行した公開鍵証明証を参照し（Ｓ４）、その証明証を発行した証明機関を知り、かつその機関証明証を取得し（Ｓ５）、その発行証明機関より上位の証明機関

があるかを調べ（Ｓ６）、あればステップＳ５に戻って、その機関証明証を発行した証明機関を知るとともにその機関証明証を取得し、機関証明証を発行した証明機関が最上位に到達すると、それまでに取得した機関証明証の検証処理に移る。

【００２０】つまり対象証明機関に対する機関証明証の署名を、その２の証明証を発行した証明機関に対する機関証明証内にある公開鍵で検証し（Ｓ７）、更にその発行証明機関の機関証明証の署名を、その証明証を発行した証明機関に対する機関証明証内の公開鍵を用いて検証し（Ｓ８）、機関証明証の署名の検証が最上位の証明機関の公開鍵により行ったかを調べ（Ｓ９）、そうでなければステップＳ８に戻り、機関証明証の署名の検証を順次上位の証明機関について行い、最上位の証明機関の公開鍵による検証が行われ、全ての検証に合格すると、対象証明機関に対する機関証明証からその対象証明機関の公開鍵及び公開情報を取り出し（Ｓ１０）、その取り出した公開鍵及び公開情報に、これに対する自証明機関の署名を付けて機関証明証を作成して記憶部２１に記憶するとともに要求ユーザ端末へ送信する（Ｓ１１）。

【００２１】

【発明の効果】以上述べたようにこの発明によれば、

① ユーザが、自分の証明証を発行した証明機関と異なる証明機関から発行されている通信相手の公開鍵証明証の正当性を検証する際に、そのユーザ端末自身で信頼の木構造を順次辿って複数の証明証を検証することなく、各証明機関が発行する間接認証による証明証のみを用いて確実に検証できることから、ユーザの検証処理が軽減される。

【００２２】さらに、

② ユーザが検証処理の際に用いる間接認証による証明証の取得要求は、ユーザ自身の証明証の発行元証明機関のみに対して行われることから、木構造の上位の証明機関にアクセスが集中することを回避することができる。

【図面の簡単な説明】

【図１】Ａはこの発明を適用したシステム構成例を示すブロック図、Ｂはユーザ端末１４Ｂの認証処理手順の例を示す流れ図である。

【図２】この発明において証明機関の公開鍵の認証要求を受けた証明機関の処理手順の例を示す流れ図。

【図３】同一の証明機関が発行した公開鍵証明証でのユーザ間通信における認証を説明するためのシステム構成例を示すブロック図。

【図４】Ａは異なる証明機関により認証された公開鍵証明証によるユーザ間の通信における認証を説明するためのシステム構成例を示す図、Ｂはその公開鍵認証手順の例を示す図である。

【図１】

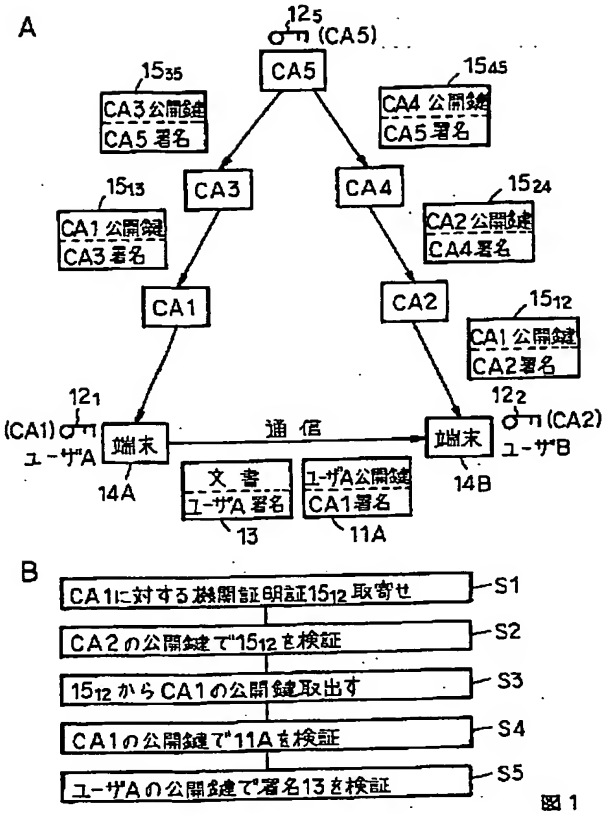


図１

【図３】

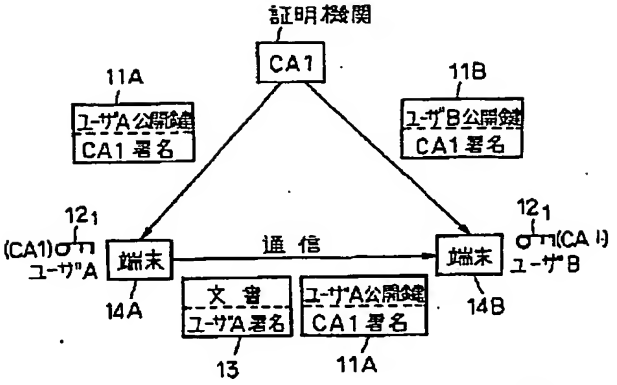


図３

【図４】

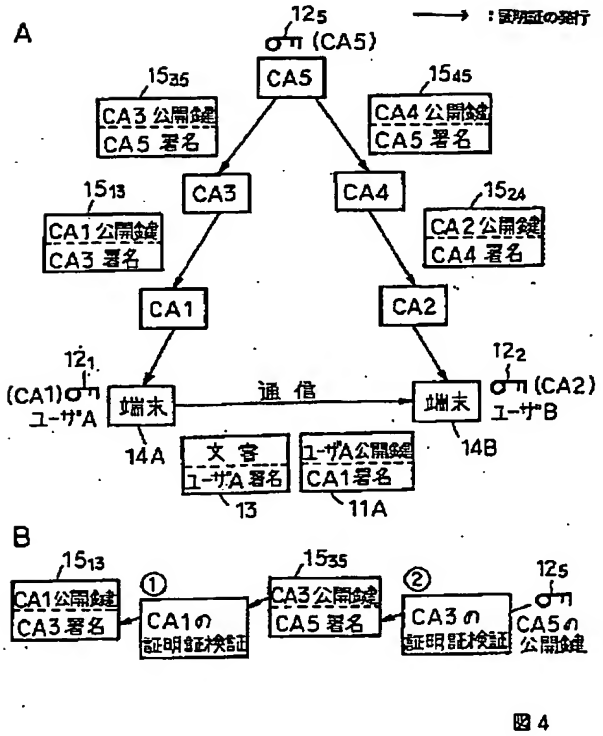


図４

【図２】

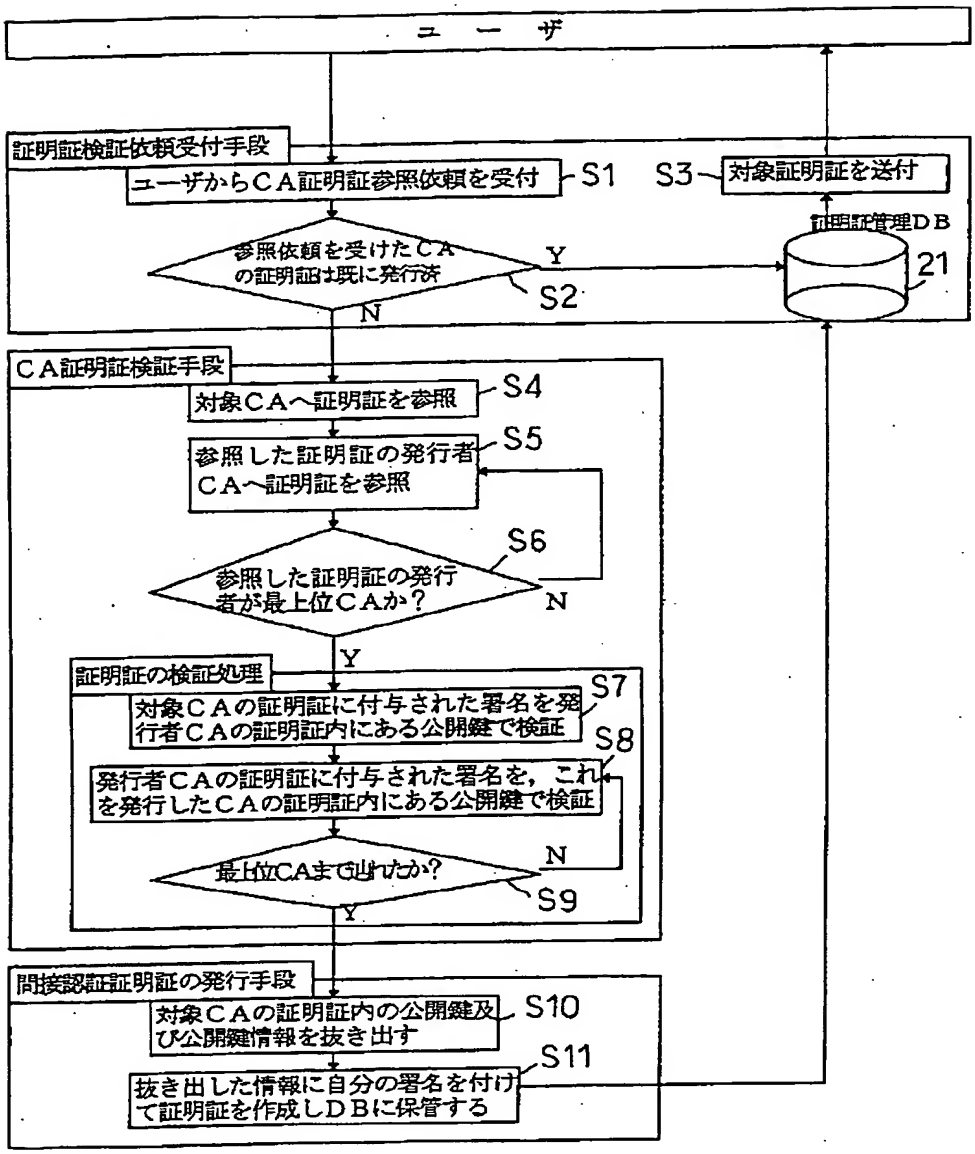

ユーザ
証明証検証依頼受付手段
ユーザからＣＡ証明証参照依頼を受付
S1
S3
対象証明証を送付
証明証管理ＤＢ
21
参照依頼を受けたＣＡの証明証は既に発行済
Y
S2
N
ＣＡ証明証検証手段
対象ＣＡへ証明証を参照
S4
参照した証明証の発行者ＣＡへ証明証を参照
S5
S6
参照した証明証の発行者が最上位ＣＡか？
N
Y
証明証の検証処理
対象ＣＡの証明証に付与された署名を発行者ＣＡの証明証内にある公開鍵で検証
S7
S8
発行者ＣＡの証明証に付与された署名を，これを発行したＣＡの証明証内にある公開鍵で検証
最上位CAまで辿れたか?
N
S9
Y
間接認証証明証の発行手段
対象ＣＡの証明証内の公開鍵及び公開鍵情報を抜き出す
S10
S11
抜き出した情報に自分の署名を付けて証明証を作成しＤＢに保管する

図 2